

[Web](#) [Images](#) [Maps](#) [News](#) [Products](#) [Gmail](#) [more ▾](#)
[Sign in](#)

Google

secure private e-mail mesaaging

Search

[Advanced Search](#)  
[Preferences](#)

Web

Results 1 - 10 of about 201,000 for **secure private e-mail mesaaging**. (0.20 seconds)**Sensitive customer email**

www.Voltage.com Send it securely via email No extra software required

**CertifiedMail Secure mail**

www.CertifiedMail.com E-mail Security, Tracking, Content Filter, GLB HIPAA Compliance Simple

Sponsored Links

**Secure Email Encryption**

Are PKI, S/MIME & OpenPGP Secure? Free Whitepaper examines encryption  
 www.Postini.com

**Secure Your Email**

Protect your critical business data  
 PKI Encryption made easy! \$8.50/mo.  
 www.lceSECURE.com

**Secure Mail**

Advanced, Reliable Email Services.  
 Secure Protection Against Spamming.  
 www.Rackspace.com

**Email Security Solution**

BorderWare Stops Up To 98% of Spam  
 Get an Evaluation for-Your Company!  
 www.BorderWare.com

**Secure Email Appliance**

Send Secure Email to Anyone  
 Easy Setup and Administration  
 www.cyglan.com

**Symantec Mail Security**

No risk evaluation program for SMS  
 8300 appliances; Download now!  
 www.Symantec.com

**Email Messaging marketing**

Barack Obama & 100,000 Others Chose iContact. Start a Free Trial Today!  
 www.iContact.com

**Email Encryption Tool**

Insure data security for Sarbanes-Oxley, ePHI /HIPPA GLBA  
 www.Ceelox.com

[More Sponsored Links »](#)Did you mean: **secure private email messaging****Proofpoint Web Seminar: Secure Email Communications | Email Encryption**

How Do I Protect and Secure Private Data? Email is commonly used to transmit .... The Proofpoint Secure Messaging™ module, a component of the Proofpoint ...  
 www.proofpoint.com/id/Encryptionwebinar0207/index.php?id=3 - 54k  
 - [Cached](#) - [Similar pages](#)

**Proofpoint : Proofpoint Secure Messaging | Policy-driven Email ...**

The Proofpoint Secure Messaging module adds policy-based email encryption ... Decryption (or private) keys are generated by the Proofpoint Secure Messaging ...  
 www.proofpoint.com/products/secure.php - 27k -  
[Cached](#) - [Similar pages](#)

[\[ More results from www.proofpoint.com \]](#)**Keep Your Email Secure With EasyLink's Private Email Services**

Many companies process mission-critical business messages that must be kept totally secure. EasyLink's Private Email service is completely isolated from the ...  
 www.easylink.com/products/data-messaging/private-email/ - 22k -  
[Cached](#) - [Similar pages](#)

**Information Security: PGP**

The message can only be decrypted with that person's private key. ... Vendors and proponents of secure e-mail are working to reconcile competing standards ...  
 www.upenn.edu/computing/security/pgp.html - 33k -  
[Cached](#) - [Similar pages](#)

**Cyber-Rights.net :// Free, Secure & Private Email**

Free Secure and Private Web Based Email From Cyber-Rights. ... Instant Messaging: Access to Hush Messenger, our encrypted instant messaging client ...  
 www.cyber-rights.net/ - 28k - [Cached](#) - [Similar pages](#)

**Outsourced Email Solution for Business, secure hosted email ...**

DocDeadbolt - **Secure Email** and Document Delivery Solution. Securely share and track **private email**, documents and large attachments with partners, ...  
[www.gmsi1.com/](http://www.gmsi1.com/) - 15k - [Cached](#) - [Similar pages](#)

**PrivacyHarbor™ - Secure Business Email Solution**

PrivacyHarbor™ Business **Messaging**. **Private email**, **secure** messages, ...  
PrivacyHarbor™ is a **secure** business-class **messaging** solution that's affordable! ...  
[www.privacyharbor.com/secure-business-messaging.html](http://www.privacyharbor.com/secure-business-messaging.html) - 24k - [Cached](#) - [Similar pages](#)

**www.KeptPrivate.com - faq - secure email**

**Secure email** service with both Web and POP/IMAP access. ... In summary, "Closed Loop" **private messaging** means that as a KeptPrivate.com subscriber I can ...  
[www.keptprivate.com/faq.php](http://www.keptprivate.com/faq.php) - 10k - [Cached](#) - [Similar pages](#)

**Email Hosting, Exchange Hosting, Hosted Exchange Business Email ...**

and Hosted **Email** services for your business **email** and mobile **messaging** needs. ...  
**Secure Email** and **Email** Compliance with Exchange Hosting ...  
[www.usa.net/](http://www.usa.net/) - 35k - [Cached](#) - [Similar pages](#)

**Cool Solutions: Secure Messaging, Part 1: The Challenges of Email ...**

Tovaris is our newest **secure messaging** partner. They are an **e-mail** privacy ... The **private** key is never shared by the user, and it is typically encrypted ...  
[www.novell.com/coololutions/trench/9395.html](http://www.novell.com/coololutions/trench/9395.html) - 21k - [Cached](#) - [Similar pages](#)

Did you mean to search for: **secure private email messaging**

1 2 3 4 5 6 7 8 9 10 **Next**

Download [Google Pack](#): free essential software for your PC

---

[Search within results](#) | [Language Tools](#) | [Search Tips](#) | [Dissatisfied?](#) [Help us improve](#)

---

©2007 Google - [Google Home](#) - [Advertising Programs](#) - [Business Solutions](#) - [About Google](#)

[Web](#) [Images](#) [Maps](#) [News](#) [Products](#) [Gmail](#) [more ▾](#)
[Sign in](#)

Google

secure private email messaging

Search

[Advanced Search](#)  
[Preferences](#)

Web

Results 1 - 10 of about 232,000 for **secure private email messaging**. (0.23 seconds)**Sensitive customer email**

[www.Voltage.com](#) Send it securely via email No extra software required

**Presensoft™ IM Caller ID**

[www.presensoft.com](#) Protect proprietary company data with bi-directional authentication.

**Cyber-Rights.net :// Free, Secure & Private Email**

Free **Secure** and **Private** Web Based **Email** From Cyber-Rights. ...  
**Instant Messaging:** Access to Hush Messenger, our encrypted instant messaging client ...

[www.cyber-rights.net/](#) - 28k - [Cached](#) - [Similar pages](#)

**Keep Your Emails Secure, Private and Anonymous - About Email**

Keep Your Emails **Secure**, **Private** and Anonymous ... By merely opening an **email message**, you may be revealing a lot about yourself.

[email.about.com/od/staysecureandprivate/](#)

[Keep\\_Your\\_Emails\\_Secure\\_Private\\_and\\_Anonymous.htm](#) - 18k - [Cached](#) - [Similar pages](#)

**WebLOQ Creates Private Domains to Secure E-Mail**

WebLOQ **Private Email** is available for enterprises and as a hosted ....  
 Want an easy way to keep up collaboration and **messaging** news, reviews and opinions? ...

[www.eweek.com/article2/0,1895,2175221,00.asp](#) - 101k -

[Cached](#) - [Similar pages](#)

**Lifescape Medical Associates. Member of the Medem Network ...**

Lifescape Medical Associates. Member of the Medem Network: Connecting Physicians and Patients Online.

[www.lifescapemed.medem.com/](#) - 43k - [Cached](#) - [Similar pages](#)

**Private Email Downloads - Secure email for everyone. It is an easy ...**

It is an easy-to-use next generation **secure email** technology. .... Your **private email message** are not so **private**. When attached to an **email**, ...

[pcwin.com/popular/Private\\_Email-1.htm](#) - 68k - [Cached](#) - [Similar pages](#)

**Proofpoint : Proofpoint Secure Messaging | Policy-driven Email ...**

The Proofpoint **Secure Messaging** module adds policy-based **email** encryption ...

Decryption (or **private**) keys are generated by the Proofpoint **Secure Messaging** ...

[www.proofpoint.com/products/secure.php](#) - 27k - [Cached](#) - [Similar pages](#)

**Public/Private/Invitation Email Address Based Secure Anti-Spam ...**

The **Secure Anti-Spam Email Protocol (SASEP)** as proposed by this invention is based on ... [0009] For each **email message** received on **private email** address, ...

[www.freepatentsonline.com/20050235041.html](#) - 35k - [Cached](#) - [Similar pages](#)

Sponsored Links

**Secure Email**

Advanced, Reliable **Email** Services.

**Secure** Protection Against Spamming.

[www.Rackspace.com](#)

**CertifiedMail Secure mail**

**E-mail** Security, Tracking, Content

Filter, GLB HIPAA Compliance Simple

[www.CertifiedMail.com](#)

**Secure Your Email**

Protect your critical business data

PKI Encryption made easy! \$8.50/mo.

[www.lceSECURE.com](#)

**Email Encryption Software**

More **secure** than PKI solutions

works-with-Outlook

[www.Ceelox.com](#)

**Enterprise Email Platform**

All-in-One Inbound, Outbound and

Internal **Email** Protection. See How.

[www.Sendmail.com](#)

**Information Security: PGP**

The **message** can only be decrypted with that person's **private** key. ... Vendors and proponents of **secure e-mail** are working to reconcile competing standards ...  
[www.upenn.edu/computing/security/pgp.html](http://www.upenn.edu/computing/security/pgp.html) - 33k - [Cached](#) - [Similar pages](#)

**Keep Your Email Secure With EasyLink's Private Email Services**

Many companies process mission-critical business messages that must be kept totally **secure**. EasyLink's **Private Email** service is completely isolated from the ...  
[www.easylink.com/products/data-messaging/private-email/](http://www.easylink.com/products/data-messaging/private-email/) - 22k - [Cached](#) - [Similar pages](#)

**Lockbin - send private, secure messages, easily**

Email isn't **secure**. Even if you connect to your **email** server using SSL, ... **Email**). He / She will not be able to read the **email message** without it! ...  
[www.lockbin.com/](http://www.lockbin.com/) - 27k - [Cached](#) - [Similar pages](#)

[1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#)    **[Next](#)**

Try [Google Desktop](#): search your computer as easily as you search the web.

---

[Search within results](#) | [Language Tools](#) | [Search Tips](#) | [Dissatisfied? Help us improve](#)

---

©2007 Google - [Google Home](#) - [Advertising Programs](#) - [Business Solutions](#) - [About Google](#)

[Web](#) [Images](#) [Maps](#) [News](#) [Products](#) [Gmail](#) [more ▾](#)[Sign in](#)

Google

secure private email messaging

Search

[Advanced Search](#)  
[Preferences](#)

Web

Results 11 - 20 of about 230,000 for **secure private email messaging**. (0.18 seconds)**Secure e-mail system - US Patent 6584564**

(d) decrypting the **secure e-mail** at said receiver based on said **message** key, ... password is derived from a **private** password provided by said receiver, ...  
[www.patentstorm.us/patents/6584564-claims.html](http://www.patentstorm.us/patents/6584564-claims.html) - 21k -  
[Cached](#) - [Similar pages](#)

**Free email, email account, free email address, email service ...**

BigString **email** service for **secure**, **private**, recallable, erasable **email**. ... **Message** Sorting, check, check, check. Fun **Email** Effects, check, check, check ...  
[www.bigstring.com/](http://www.bigstring.com/) - 26k - [Cached](#) - [Similar pages](#)

**Outsourced Email Solution for Business, secure hosted email ...**

DocDeadbolt - **Secure Email** and Document Delivery Solution. Securely share and track **private email**, documents and large attachments with partners, ...  
[www.gmsi1.com/](http://www.gmsi1.com/) - 15k - [Cached](#) - [Similar pages](#)

**Mac OS X 10.3: Mail - How to Use a Secure Email Signing ...**

Learn how Mail in Mac OS X Panther can import a **secure email** signing ... To send a signed **message**, you only need a **private** key for the sending **email** address ...  
[docs.info.apple.com/article.html?artnum=25555](http://docs.info.apple.com/article.html?artnum=25555) - 17k -  
[Cached](#) - [Similar pages](#)

**Using PGP to Secure Your SOHO Email**

When you receive my **email**, you can use your **private** key to decrypt the **message**. In addition to securing **email** to maintain privacy, you can use your **private** ...  
[www.windowstpro.com/Article/ArticleID/20696/20696.html](http://www.windowstpro.com/Article/ArticleID/20696/20696.html) -  
[Similar pages](#)

**IMAP Hosting, SSL, PGP Encryption, SSL IMAP Email, Corporate Email ...**

Find out more about **Private** Labeling. Listen to Our Clients: "I spent weeks scouring the Internet for companies that offer a complete set of **secure email** ...  
[luxsci.com/extranet/articles/email-security.html](http://luxsci.com/extranet/articles/email-security.html) - 44k -  
[Cached](#) - [Similar pages](#)

**www.KeptPrivate.com - faq - secure email**

**Secure email** service with both Web and POP/IMAP access. ... In summary, "Closed Loop" **private messaging** means that as a KeptPrivate.com subscriber I can ...  
[www.keptprivate.com/faq.php](http://www.keptprivate.com/faq.php) - 10k - [Cached](#) - [Similar pages](#)

## Sponsored Links

**Secure Email**

Advanced, Reliable **Email** Services.  
**Secure** Protection Against Spamming.  
[www.Rackspace.com](http://www.Rackspace.com)

**Secure Email Encryption**

Are PKI, S/MIME & OpenPGP **Secure**?  
Free Whitepaper examines encryption  
[www.Postini.com](http://www.Postini.com)

**Secure Email Appliance**

Send **Secure Email** to Anyone  
Easy Setup and Administration  
[www.cyglan.com](http://www.cyglan.com)

**Email Encryption Software**

More **secure** than PKI solutions  
works with Outlook  
[www.Ceelox.com](http://www.Ceelox.com)

**Secure Enterprise Email**

In Compliance with HIPAA, SB 1386, NYSE404, GLBA, PCI, Etc. Whitepaper  
[www.Sendmail.com](http://www.Sendmail.com)

**Secure messaging**

Best-In-Class **E-mail** Protection For Companies of All Sizes. Learn More!  
[www.McAfee.com](http://www.McAfee.com)

**Need to secure email?**

Podcast from encryption leader discusses **email** security options  
[www.entrust.com](http://www.entrust.com)

**Jabber Secure IM**

Gives enterprises control over IM operation and content.  
[www.jabber.com](http://www.jabber.com)

**XSPMail :: Home :: Private, Secure Email and More**

XSPMail is a **secure, private email** service built with the worlds leading ... can read your encrypted **email**, since each **message** is uniquely encoded before it ...

[www.xspmail.com/](http://www.xspmail.com/) - 15k - [Cached](#) - [Similar pages](#)

**About certificates and cryptographic e-mail messaging in Outlook ...**

Outlook 2003 uses certificates in cryptographic **e-mail messaging** to help provide more **secure** communications. To use cryptography when you send and receive ...

[office.microsoft.com/en-us/outlook/HP010461711033.aspx](http://office.microsoft.com/en-us/outlook/HP010461711033.aspx) - 54k - [Cached](#) - [Similar pages](#)

**anywhere - secure private file sharing**

after you receive you login information by **email** login to your account to change ... **email** share links to files, **secure** and **private** >> remote file storage ...

[www.filessharinganywhere.com/fsa/index.jsp](http://www.filessharinganywhere.com/fsa/index.jsp) - 21k - [Cached](#) - [Similar pages](#)

**Previous** [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [11](#) **Next**

---

---

[Search within results](#) | [Language Tools](#) | [Search Tips](#)

---

©2007 Google - [Google Home](#) - [Advertising Programs](#) - [Business Solutions](#) - [About Google](#)

[Web](#) [Images](#) [Maps](#) [News](#) [Products](#) [Gmail](#) [more ▾](#)[Sign in](#)

Google

secure private email messaging

Search

[Advanced Search](#)  
[Preferences](#)

Web

Results 21 - 30 of about 232,000 for **secure private email messaging**. (0.13 seconds)

### Neomailbox Secure Email :: Encryption Security -- Email Encryption ...

The sender signs the **message** using her **private** key, and this signature can only be ... With our offshore **secure email** service you also receive access to two ...

[www.neomailbox.com/ssl\\_session\\_encryption.html](http://www.neomailbox.com/ssl_session_encryption.html) - 28k -

[Cached](#) - [Similar pages](#)

### PrivacyHarbor™ - Secure Business Email Solution

PrivacyHarbor™ Business **Messaging**. **Private email**, **secure** messages, ... PrivacyHarbor™ is a **secure** business-class **messaging** solution that's affordable! ...

[www.privacyharbor.com/secure-business-messaging.html](http://www.privacyharbor.com/secure-business-messaging.html) - 24k -

[Cached](#) - [Similar pages](#)

### [PDF] Secure Messaging for Your Enterprise E-mail - White Paper

File Format: PDF/Adobe Acrobat - [View as HTML](#)

This is in sharp contrast to other **secure e-mail** alternatives that require .... own **private** key, thus ensuring to the recipient that the **message** really came ...

[www.verisign.com/static/006972.pdf](http://www.verisign.com/static/006972.pdf) - [Similar pages](#)

### Cool Solutions: Secure Messaging, Part 1: The Challenges of Email ...

Tovaris is our newest **secure messaging** partner. They are an **e-mail** privacy ... The **private** key is never shared by the user, and it is typically encrypted ...

[www.novell.com/coolsolutions/trench/9395.html](http://www.novell.com/coolsolutions/trench/9395.html) - 21k -

[Cached](#) - [Similar pages](#)

### RelayHealth - Secure Connectivity Solutions for Healthcare

Hospitals, Pharmacies and Partners, learn more. **Message** for Patients. Patients. RelayHealth is a **secure**, **private** way to communicate with your doctor online. ...

<https://www.relayhealth.com/> - 12k - [Cached](#) - [Similar pages](#)

### Secure Enterprise & Corporate Instant Messaging (IM)

Chat also offers hyperlinks, **private messaging** to individual participants and session logging; Better, more **secure** and more immediate than **e-mail** ...

[www.wiredred.com/secure-messaging/](http://www.wiredred.com/secure-messaging/) - 26k -

[Cached](#) - [Similar pages](#)

### Identity-Based Encryption

Note that unlike the existing **secure e-mail** infrastructure, Alice can send ... key corresponding to this IBE encryption key and then decrypt the **message**. ...

[crypto.stanford.edu/ibe/](http://crypto.stanford.edu/ibe/) - 13k - [Cached](#) - [Similar pages](#)

### Sponsored Links

#### Secure Messaging

Authenticate & encrypt your instant **messaging**. Advanced IM security.  
[www.presensoft.com](http://www.presensoft.com)

#### Secure Email

Advanced, Reliable **Email** Services.  
**Secure** Protection Against Spamming.  
[www.Rackspace.com](http://www.Rackspace.com)

#### CertifiedMail Secure mail

**E-mail** Security, Tracking, Content Filter, GLB HIPAA Compliance Simple  
[www.CertifiedMail.com](http://www.CertifiedMail.com)

#### Secure Email Encryption

Are PKI, S/MIME & OpenPGP **Secure**?  
Free Whitepaper examines encryption  
[www.Postini.com](http://www.Postini.com)

#### Secure Your Email

Protect your critical business data  
PKI Encryption made easy! \$8.50/mo.  
[www.lceSECURE.com](http://www.lceSECURE.com)

#### Email Encryption Tool

Insure data security for  
Sarbanes-Oxley, ePHI /HIPPA GLBA  
[www.Ceelox.com](http://www.Ceelox.com)

#### Secure Enterprise Email

In Compliance with HIPAA, SB 1386, NYSE404, GLBA, PCI, Etc. Whitepaper  
[www.Sendmail.com](http://www.Sendmail.com)

#### Jabber Secure IM

Gives enterprises control over  
IM operation and content.  
[www.jabber.com](http://www.jabber.com)

**Instant messaging - Wikipedia, the free encyclopedia**

Instant **messaging** has proven to be similar to personal computers, e-mail, ... **secure**, productive instant **messaging** capabilities to their employees. ...

en.wikipedia.org/wiki/Instant\_messaging - 61k - [Cached](#) - [Similar pages](#)

**Hushmail - Free Email with Privacy - About**

Welcome to Hushmail.com, the world's most **secure** free email service! ... The message key can only be decrypted by using the recipient's **private** key. ...

www.hushmail.com/about-how - 21k - [Cached](#) - [Similar pages](#)

**Total Control Over Email Security**

TFS **Secure Messaging** provides total control of email and web ... more TFS **Secure Messaging** PCs to be securely connected over a Virtual **Private** Network (VPN) ...

www.secure-message.com/Email\_security.htm - 38k - [Cached](#) - [Similar pages](#)

**Previous** [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [11](#) [12](#) **Next**

---

[Search within results](#) | [Language Tools](#) | [Search Tips](#)

---

©2007 Google - [Google Home](#) - [Advertising Programs](#) - [Business Solutions](#) - [About Google](#)





USPTO

[Subscribe \(Full Service\)](#) [Register \(Limited Service, Free\)](#) [Login](#)

 Search: ☒ The ACM Digital Library ☐ The Guide



THE ACM DIGITAL LIBRARY


[Feedback](#) [Report a problem](#) [Satisfaction survey](#)
Terms used: secure email message

Found 15,167 of 215,737

Sort results by

Display results

☒ [Save results to a Binder](#)
☒ [Search Tips](#)
☐ Open results in a new window
Try an [Advanced Search](#)Try this search in [The ACM Guide](#)

Results 1 - 20 of 200

Result page: [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [next](#)

Best 200 shown.

Relevance scale ☐ ☐ ☐ ☐ ☐

# 1 [Email and security: How to make secure email easier to use](#)


 Simson L. Garfinkel, David Margrave, Jeffrey I. Schiller, Erik Nordlander, Robert C. Miller  
 April 2005 **Proceedings of the SIGCHI conference on Human factors in computing systems CHI '05**

Publisher: ACM Press

Full text available: [pdf\(419.10 KB\)](#)
 Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

Cryptographically protected email has a justly deserved reputation of being difficult to use. Based on an analysis of the PEM, PGP and S/MIME standards and a survey of 470 merchants who sell products on Amazon.com, we argue that the vast majority of Internet users can start enjoying digitally signed email today. We present suggestions for the use of digitally signed mail in e-commerce and simple modifications to webmail systems that would significantly increase integrity, privacy and authorship ...

**Keywords:** e-commerce, user interaction design, user studies

# 2 [Secure external references in multimedia email messages](#)


 Burkhard Wiegel  
 January 1996 **Proceedings of the 3rd ACM conference on Computer and communications security CCS '96**

Publisher: ACM Press

Full text available: [pdf\(1.27 MB\)](#)
 Additional Information: [full citation](#), [references](#), [index terms](#)

# 3 [Certified mail: the next challenge for secure messaging](#)


 Rolf Oppliger  
 August 2004 **Communications of the ACM**, Volume 47 Issue 8

Publisher: ACM Press

Full text available: [pdf\(88.44 KB\)](#)
[html\(25.71 KB\)](#)

 Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

The lack of evidence for message receipt is a missing piece of the infrastructure required for the more professional use of email.

4

# [Security architecture: BPEL orchestration of secure webmail](#)

-  Saket Kaushik, Duminda Wijesekera, Paul Ammann  
November 2006 **Proceedings of the 3rd ACM workshop on Secure web services SWS '06**

**Publisher:** ACM Press

Full text available:  [pdf\(422.08 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

WebMail proposes to migrate existing SMTP-based mail systems to Web-Services. We show how a verifiably-correct, generic mail service that enables extensions of SMTP-based standard mail use cases that avoids known misuse cases can be specified using WSDL and orchestrated using BPEL.

**Keywords:** BPEL, SMTP misuse cases, SMTP use cases, WSEmail, verification, webmail

5 Johnny 2: a user test of key continuity management with S/MIME and Outlook



**Express**

Simson L. Garfinkel, Robert C. Miller

July 2005 **Proceedings of the 2005 symposium on Usable privacy and security SOUPS '05**

**Publisher:** ACM Press

Full text available:  [pdf\(665.63 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

Secure email has struggled with significant obstacles to adoption, among them the low usability of encryption software and the cost and overhead of obtaining public key certificates. Key continuity management (KCM) has been proposed as a way to lower these barriers to adoption, by making key generation, key management, and message signing essentially automatic. We present the first-user-study of KCM-secured email, conducted on naïve users who had no previous experience with secure email. Our ...

**Keywords:** Usability, e-commerce, user interaction design, user studies

6 Security for Web Applications and P2P: Certified email with a light on-line trusted third party: design and implementation



Martín Abadi, Neal Glew

May 2002 **Proceedings of the 11th international conference on World Wide Web WWW '02**

**Publisher:** ACM Press

Full text available:  [pdf\(189.19 KB\)](#) Additional Information: [full citation](#), [abstract](#), [citations](#), [index terms](#)

This paper presents a new protocol for certified email. The protocol aims to combine security, scalability, easy implementation, and viable deployment. The protocol relies on a light on-line trusted third party; it can be implemented without any special software for the receiver beyond a standard email reader and web browser, and does not require any public-key infrastructure.

7 Enabling email confidentiality through the use of opportunistic encryption

Simson L. Garfinkel

May 2003 **Proceedings of the 2003 annual national conference on Digital government research dg.o '03**

**Publisher:** Digital Government Research Center

Full text available:  [pdf\(51.35 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#)

Software for encrypting email messages has been widely available for more than 15 years, but the email-using public has failed to adopt secure messaging. This failure can be explained through a combination of technical, community, and usability factors. This paper proposes a new approach to email security that employs opportunistic encryption

and a security proxy to facilitate the opportunistic exchange of keys and encryption of electronic mail. While it appears that this approach offers less se ...

8 SOUPS du jour: Facemail: showing faces of recipients to prevent misdirected email



Eric Lieberman, Robert C. Miller

July 2007 **Proceedings of the 3rd symposium on Usable privacy and security SOUPS '07**

**Publisher:** ACM Press

Full text available: [pdf\(615.51 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Users occasionally send email to the wrong recipients -- clicking Reply To All instead of Reply, mistyping an email address, or guessing an email address and getting it wrong - and suffer violations of security or privacy as a result. Facemail is an extension to a webmail system that aims to alleviate this problem by automatically displaying pictures of the selected recipients in a peripheral display, while the user is composing an email message. We describe techniques for obtaining faces fro ...

**Keywords:** email, errors, privacy, reply to all, security

9 (How) can mobile agents do secure electronic transactions on untrusted hosts? A survey of the security issues and the current solutions



Joris Claessens, Bart Preneel, Joos Vandewalle

February 2003 **ACM Transactions on Internet Technology (TOIT)**, Volume 3 Issue 1

**Publisher:** ACM Press

Full text available: [pdf\(197.96 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

This article investigates if and how mobile agents can execute secure electronic transactions on untrusted hosts. An overview of the security issues of mobile agents is first given. The problem of untrusted (i.e., potentially malicious) hosts is one of these issues, and appears to be the most difficult to solve. The current approaches to counter this problem are evaluated, and their relevance for secure electronic transactions is discussed. In particular, a state-of-the-art survey of mobile agen ...

**Keywords:** Mobile agent security, electronic transactions, malicious hosts

10 Security in the wild: user strategies for managing security as an everyday, practical problem

Paul Dourish, E. Grinter, Jessica Delgado de la Flor, Melissa Joseph

November 2004 **Personal and Ubiquitous Computing**, Volume 8 Issue 6

**Publisher:** Springer-Verlag

Full text available: [pdf\(227.06 KB\)](#) Additional Information: [full citation](#), [abstract](#), [citations](#), [index terms](#), [review](#)

Ubiquitous and mobile technologies create new challenges for system security. Effective security solutions depend not only on the mathematical and technical properties of those solutions, but also on people's ability to understand them and use them as part of their work. As a step towards solving this problem, we have been examining how people experience security as a facet of their daily life, and how they routinely answer the question, "is this system secure enough for what I ...

11 Accountability protocols: Formalized and verified



Giampaolo Bella, Lawrence C. Paulson

May 2006 **ACM Transactions on Information and System Security (TISSEC)**, Volume 9 Issue 2

**Publisher:** ACM Press

Full text available:  pdf(433.82 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Classical security protocols aim to achieve authentication and confidentiality under the assumption that the peers behave honestly. Some recent protocols are required to achieve their goals even if the peer misbehaves. *Accountability* is a protocol design strategy that may help. It delivers to peers sufficient evidence of each other's participation in the protocol. Accountability underlies the nonrepudiation protocol of Zhou and Gollmann and the certified email protocol of Abadi et al. Thi ...

**Keywords:** Isabelle, Nonrepudiation, certified email, inductive method, proof tools

## 12 Privacy and authentication: An effective defense against email spam laundering



Mengjun Xie, Heng Yin, Haining Wang

October 2006 **Proceedings of the 13th ACM conference on Computer and communications security CCS '06**

**Publisher:** ACM Press

Full text available:  pdf(362.04 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Laundering email spam through open-proxies or compromised PCs is a widely-used trick to conceal real spam sources and reduce spamming cost in underground email spam industry. Spammers have been plaguing the Internet by exploiting a large number of spam proxies. The facility of breaking spam laundering and deterring spamming activities close to their sources, which would greatly benefit not only email users but also victim ISPs, is in great demand but still missing. In this paper, we reveal one s ...

**Keywords:** SPRT, proxy, spam


## 13 Managing user perceptions of email privacy



Suzanne P. Weisband, Bruce A. Reinig

December 1995 **Communications of the ACM**, Volume 38 Issue 12

**Publisher:** ACM Press

Full text available:  pdf(213.15 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

Email users, expecting privacy, risk embarrassment, lawsuits, and worse.


## 14 Communication privacy: Off-the-record communication, or, why not to use PGP



Nikita Borisov, Ian Goldberg, Eric Brewer

October 2004 **Proceedings of the 2004 ACM workshop on Privacy in the electronic society WPES '04**

**Publisher:** ACM Press

Full text available:  pdf(154.87 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

Quite often on the Internet, cryptography is used to protect private, personal communications. However, most commonly, systems such as PGP are used, which use long-lived encryption keys (subject to compromise) for confidentiality, and digital signatures (which provide strong, and in some jurisdictions, legal, proof of authorship) for authenticity.

In this paper, we argue that most social communications online should have just the opposite of the above two properties; namely, they should ...


**Keywords:** deniability, perfect forward secrecy, private communication

15 The ethical and legal quandary of email privacy

 Janice C. Sipior, Burke T. Ward

December 1995 **Communications of the ACM**, Volume 38 Issue 12

**Publisher:** ACM Press

Full text available:  pdf(204.07 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

What should conscientious employees and their ethical employers expect? It's hard to say.

16 Security: Secrecy, flagging, and paranoia: adoption criteria in encrypted email

 Shirley Gaw, Edward W. Felten, Patricia Fernandez-Kelly

April 2006 **Proceedings of the SIGCHI conference on Human Factors in computing systems CHI '06**

**Publisher:** ACM Press

Full text available:  pdf(502.61 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

We consider the social context behind users' decisions about whether and when to encrypt email, interviewing a sample of users from an organization whose mission requires secrecy. Interview participants varied in their level of technical sophistication and in their involvement with secrets. We found that users saw universal, routine use of encryption as paranoid. Encryption flagged a message not only as confidential but also as urgent, so users found the encryption of mundane messages annoying. ...

**Keywords:** activism, encrypted e-mail, extended case method, security

17 Computational mail as network infrastructure for computer-supported cooperative work

 Nathaniel S. Borenstein


December 1992 **Proceedings of the 1992 ACM conference on Computer-supported cooperative work CSCW '92**

**Publisher:** ACM Press

Full text available:  pdf(911.62 KB) Additional Information: [full citation](#), [references](#), [citations](#), [index terms](#)

**Keywords:** CSCW infrastructure, active mail, electronic mail, portability, security

18 Cryptographic tools: Versatile padding schemes for joint signature and encryption

 Yevgeniy Dodis, Michael J. Freedman, Stanislaw Jarecki, Shabsi Walfish

October 2004 **Proceedings of the 11th ACM conference on Computer and communications security CCS '04**

**Publisher:** ACM Press

Full text available:  pdf(203.91 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

We propose several highly-practical and optimized constructions for joint signature and encryption primitives often referred to as *signcryption*. All our signcryption schemes, built directly from trapdoor permutations such as RSA, share features such as simplicity, efficiency, generality, near-optimal exact security, flexible and ad-hoc key management, key reuse for sending/receiving data, optimally-low message expansion, "backward" use for plain signature/encryption, long messa ...

**Keywords:** extractable commitments, feistel transform, joint signature and encryption, signcryption, universal padding schemes

**19 Session 2: Email feedback: a policy-based approach to overcoming false positives**

Saket Kaushik, William Winsborough, Duminda Wijesekera, Paul Ammann

November 2005 **Proceedings of the 2005 ACM workshop on Formal methods in security engineering FMSE '05****Publisher:** ACM PressFull text available: [pdf\(205.07 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Current email-control mechanisms, though highly effective, are prone to dropping desirable messages. This can be attributed to their coarseness in filtering out undesirable messages from desirable ones. As a result policies to control undesirable messages are often overly permissive. To allow policies to be more restrictive, the transmission mechanism must be made aware of the ways to document a message so that it is acceptable downstream, thus giving the senders a chance of meeting those requi ...

**Keywords:** constraint logic programming, email/spam control, policy advertisement, policy feedback

**20 Communication privacy: Peripheral privacy notifications for wireless networks**

Braden Kowitz, Lorrie Cranor

November 2005 **Proceedings of the 2005 ACM workshop on Privacy in the electronic society WPES '05****Publisher:** ACM PressFull text available: [pdf\(277.68 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

When using wireless networks, some chats, web searches, and other information are broadcast out onto the local network. Other users on the same network may intercept and read this information. Unfortunately, without detailed knowledge of underlying technologies, many users are unable to properly evaluate the risks involved in everyday communication tasks. This study aims to develop techniques for allowing users without technical backgrounds to form more accurate expectations of privacy. We have ...

**Keywords:** electronic communication privacy, peripheral display, privacy, privacy enhancing technologies, wireless network

Results 1 - 20 of 200

Result page: [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [next](#)

The ACM Portal is published by the Association for Computing Machinery. Copyright © 2007 ACM, Inc.  
[Terms of Usage](#) [Privacy Policy](#) [Code of Ethics](#) [Contact Us](#)

Useful downloads: [Adobe Acrobat](#) [QuickTime](#) [Windows Media Player](#) [Real Player](#)



USPTO

[Subscribe \(Full Service\)](#) [Register \(Limited Service, Free\)](#) [Login](#)Search: ☒ The ACM Digital Library ☐ The Guide

secure email message

SEARCH

THE ACM DIGITAL LIBRARY

[Feedback](#) [Report a problem](#) [Satisfaction survey](#)Terms used: secure email message

Found 15,167 of 215,737

Sort results  
by

relevance

[Save results to a Binder](#)Try an [Advanced Search](#)Try this search in [The ACM Guide](#)Display  
results

expanded form

[Search Tips](#)☐ Open results in a new  
window

Results 21 - 40 of 200

Result page: [previous](#) [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [next](#)

Best 200 shown

Relevance scale ☐ ☐ ☐ ☐ ☐

## 21 [Asynchronous health care communication](#)



E. Vance Wilson

June 2003 **Communications of the ACM**, Volume 46 Issue 6

Publisher: ACM Press

Full text available: [pdf\(104.95 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#), [review](#)  
 [html\(29.35 KB\)](#)

Patients' desire for online communication with their health care providers is likely to change the course of both telemedicine and e-health technologies.

## 22 [Dealing with disruptions: Supporting trust building in distributed groups by appropriate security technology](#)

Wolfgang Appelt, Sanjin Pajo, Wolfgang Prinz

November 2007 **Proceedings of the 2007 international ACM conference on Conference on supporting group work GROUP '07**

Publisher: ACM

Full text available: [pdf\(289.84 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

In this paper, we discuss requirements for building trust in locally distributed groups whose members co-operate via shared workspace systems. We argue that appropriate security technology should be an intrinsic part of such systems and describe a conceptual model as well as a recent extension to an existing shared workspace system that provides the respective functionality based on PGP.

**Keywords:** BSCW, security technology, trust building

## 23 [Content-triggered trust negotiation](#)



Adam Hess, Jason Holt, Jared Jacobson, Kent E. Seamons

August 2004 **ACM Transactions on Information and System Security (TISSEC)**, Volume 7 Issue 3

Publisher: ACM Press

Full text available: [pdf\(815.36 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

The focus of access control in client/server environments is on protecting sensitive server resources by determining whether or not a client is authorized to access those resources.

The set of resources is usually static, and an access control policy associated with each resource specifies who is authorized to access the resource. In this article, we turn the traditional client/server access control model on its head and address how to protect the sensitive content that clients disclose to and r ...

**Keywords:** Trust negotiation, access control, authentication, credentials

24 Key management: Hardware-rooted trust for secure key management and transient trust

Jeffrey S. Dwoskin, Ruby B. Lee

October 2007 **Proceedings of the 14th ACM conference on Computer and communications security CCS '07**

**Publisher:** ACM

Full text available:  [pdf\(520.62 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

We propose minimalist new hardware additions to a microprocessor chip that protect cryptographic keys in portable computing devices which are used in the field but owned by a central authority. Our *authority-mode architecture* has trust rooted in two critical secrets: a Device Root Key and a Storage Root Hash, initialized in the device by the trusted authority. Our architecture protects trusted software, bound to the device, which can use the root secrets to protect other sensitive info ...

**Keywords:** emergency response, hardware policy enforcement, key management, secret protection (sp), secure processors, transient trust

25 Intrusion detection and response: MET: an experimental system for Malicious Email Tracking

Manasi Bhattacharyya, Shlomo HersHKop, Eleazar Eskin

September 2002 **Proceedings of the 2002 workshop on New security paradigms NSPW '02**

**Publisher:** ACM Press

Full text available:  [pdf\(790.18 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

Despite the use of state of the art methods to protect against malicious programs, they continue to threaten and damage computer systems around the world. In this paper we present MET, the Malicious Email Tracking system, designed to automatically report statistics on the flow behavior of malicious software delivered via email attachments both at a local and global level. MET can help reduce the spread of malicious software worldwide, especially self-replicating viruses, as well as provide furth ...

**Keywords:** anti-virus, email attachment, email tracking, virus detection

26 Securing the commercial Internet

Anish Bhimani

June 1996 **Communications of the ACM**, Volume 39 Issue 6

**Publisher:** ACM Press

Full text available:  [pdf\(1.14 MB\)](#) Additional Information: [full citation](#), [references](#), [citations](#), [index terms](#), [review](#)

27 New email security infrastructure

Martin Ferris




August 1994 **Proceedings of the 1994 workshop on New security paradigms NSPW '94**

**Publisher:** IEEE Computer Society Press

Full text available:  [pdf\(503.94 KB\)](#) Additional Information: [full citation](#), [abstract](#), [index terms](#)


This paper addresses the problem of analysing an information system for security flaws or vulnerabilities in a way that is analogous to the analysis of a safety-critical system. In particular, instead of adopting the approach that security is a property that must be proved to hold (fault avoidance), it shows how to analyse a system for possible security failures so that fault prevention, tolerance, recovery or even fault acceptance techniques can be chosen where appropriate.

28 Short papers: Defending email communication against profiling attacks

 Philippe Golle, Ayman Farahat

October 2004 **Proceedings of the 2004 ACM workshop on Privacy in the electronic society WPES '04**


**Publisher:** ACM Press

Full text available:  [pdf\(80.52 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

We define message privacy against a <i>profiling</i> adversary, whose goal is to classify a population of users into categories according to the messages they exchange. This adversary models the most common privacy threat against email communication. We propose a protocol that protects senders and receivers of email messages from profiling attacks.


**Keywords:** email, encryption, privacy, profiling

29 Security: Developing a public key infrastructure for use in a teaching laboratory

 Phillip T. Rawles, Kristoffer A. Baker

October 2003 **Proceedings of the 4th conference on Information technology curriculum CITC4 '03**


**Publisher:** ACM Press

Full text available:  [pdf\(226.86 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

Founded on the principle of easy information interchange the Internet is an inherently unsafe communication medium. Despite this inherent insecurity electronic mail continues to grow as a key communication technology. Individuals and businesses both large and small have come to rely on electronic mail. Fortunately technologies have evolved that address the lack of security in the base Internet electronic mail standards. Through the use of Public Key Infrastructure (PKI) technologies it is possib ...

**Keywords:** active directory, certificate authority, digital certificate, email, microsoft exchange, microsoft outlook, public key infrastructure

30 Inside risks: Risks in email security

 Albert Levi, Çetin Kaya Koç

August 2001 **Communications of the ACM**, Volume 44 Issue 8

**Publisher:** ACM Press

Full text available:  [pdf\(49.07 KB\)](#)  [html\(7.68 KB\)](#) Additional Information: [full citation](#), [citations](#), [index terms](#)

**31** Communication privacy: Secure off-the-record messaging

Mario Di Raimondo, Rosario Gennaro, Hugo Krawczyk

November 2005 **Proceedings of the 2005 ACM workshop on Privacy in the electronic society WPES '05**

Publisher: ACM Press

Full text available: pdf(181.59 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

At the 2004 Workshop on Privacy in the Electronic Society (WPES), Borisov, Goldberg and Brewer, presented "Off the Record Messaging" (OTR), a protocol designed to add end-to-end security and privacy to Instant Messaging protocols. An open-source implementation of OTR is available and has achieved considerable success. In this paper we present a security analysis of OTR showing that, while the overall concept of the system is valid and attractive, the protocol suffers from security shortcomings du ...

**Keywords:** authentication, deniability, instant messaging, perfect forward secrecy**32** Dynamic Access Control: An access control model for dynamic client-side content

Adam Hess, Kent E. Seamons

June 2003 **Proceedings of the eighth ACM symposium on Access control models and technologies SACMAT '03**

Publisher: ACM Press

Full text available: pdf(608.50 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

The focus of access control in client/server environments is on protecting sensitive server resources by determining whether or not a client is authorized to access those resources. The set of resources are usually static, and an access control policy associated with each resource specifies who is authorized to access the resource. In this paper, we turn the traditional client/server access control model on its head, and address how to protect the sensitive content that clients disclose to serve ...

**Keywords:** access control, authentication, credentials, trust negotiation**33** Social phishing

Tom N. Jagatic, Nathaniel A. Johnson, Markus Jakobsson, Filippo Menczer

October 2007 **Communications of the ACM**, Volume 50 Issue 10

Publisher: ACM

Full text available: pdf(204.74 KB) html(33.37 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Sometimes a "friendly" email message tempts recipients to reveal more online than they otherwise would, playing right into the sender's hand.

**34** Verifiable encryption of digital signatures and applications

Giuseppe Ateniese

February 2004 **ACM Transactions on Information and System Security (TISSEC)**, Volume 7 Issue 1

Publisher: ACM Press


Full text available: pdf(258.12 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

This paper presents a new simple schemes for verifiable encryption of digital signatures. We make use of a trusted third party (TTP) but in an *optimistic* sense, that is, the TTP takes part in the protocol only if one user cheats or simply crashes. Our schemes can be

used as primitives to build efficient fair exchange and certified e-mail protocols.

**Keywords:** Certified e-mail, contract signing, digital signatures, fair exchange, proof of knowledge, public-key cryptography

35 Improved proxy re-encryption schemes with applications to secure distributed storage

 Giuseppe Ateniese, Kevin Fu, Matthew Green, Susan Hohenberger  
February 2006 **ACM Transactions on Information and System Security (TISSEC)**, Volume 9 Issue 1


**Publisher:** ACM Press

Full text available:  [pdf\(331.59 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

In 1998, Blaze, Bleumer, and Strauss (BBS) proposed an application called *atomic proxy re-encryption*, in which a semitrusted proxy converts a ciphertext for Alice into a ciphertext for Bob *without* seeing the underlying plaintext. We predict that fast and secure re-encryption will become increasingly popular as a method for managing encrypted file systems. Although efficiently computable, the wide-spread adoption of BBS re-encryption has been hindered by considerable security risks. ...

**Keywords:** Proxy re-encryption, bilinear maps, double decryption, key translation

36 Consistent, yet anonymous, Web access with LPWA

 Eran Gabber, Phillip B. Gibbons, David M. Kristol, Yossi Matias, Alain Mayer  
February 1999 **Communications of the ACM**, Volume 42 Issue 2

**Publisher:** ACM Press

Full text available:  [pdf\(207.80 KB\)](#)  [html\(30.92 KB\)](#) Additional Information: [full citation](#), [references](#), [citations](#), [index terms](#)

37 Fine-grained control of security capabilities

 Dan Boneh, Xuhua Ding, Gene Tsudik  
February 2004 **ACM Transactions on Internet Technology (TOIT)**, Volume 4 Issue 1


**Publisher:** ACM Press

Full text available:  [pdf\(128.09 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

We present a new approach for fine-grained control over users' security privileges (fast revocation of credentials) centered around the concept of an on-line semi-trusted mediator (SEM). The use of a SEM in conjunction with a simple threshold variant of the RSA cryptosystem (mediated RSA) offers a number of practical advantages over current revocation techniques. The benefits include simplified validation of digital signatures, efficient certificate revocation for legacy systems and fast revocat ...

**Keywords:** Certificate Revocation, Digital Signatures, Public Key Infrastructure

38 Catching phish: Decision strategies and susceptibility to phishing

 Julie S. Downs, Mandy B. Holbrook, Lorrie Faith Cranor  
July 2006 **Proceedings of the second symposium on Usable privacy and security SOUPS '06**

**Publisher:** ACM Press

Full text available:  [pdf\(266.61 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Phishing emails are semantic attacks that con people into divulging sensitive information

using techniques to make the user believe that information is being requested by a legitimate source. In order to develop tools that will be effective in combating these schemes, we first must know how and why people fall for them. This study reports preliminary analysis of interviews with 20 non-expert computer users to reveal their strategies and understand their decisions when encountering possibly suspi ...

**Keywords:** mental models, phishing, qualitative methods

39 Experiences in building and operating ePOST, a reliable peer-to-peer application

Alan Mislove, Ansley Post, Andreas Haeberlen, Peter Druschel

April 2006 **ACM SIGOPS Operating Systems Review , Proceedings of the ACM SIGOPS/EuroSys European Conference on Computer Systems 2006 EuroSys '06**, Volume 40 Issue 4


**Publisher:** ACM

Full text available:  pdf(382.48 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Peer-to-peer (p2p) technology can potentially be used to build highly reliable applications without a single point of failure. However, most of the existing applications, such as file sharing or web caching, have only moderate reliability demands. Without a challenging proving ground, it remains unclear whether the full potential of p2p systems can be realized. To provide such a proving ground, we have designed, deployed and operated a p2p-based email system. We chose email because users depend o ...

**Keywords:** decentralized systems, electronic mail, peer-to-peer, reliability

40 Recipes for disaster: Googling considered harmful

 Gregory Conti

September 2006 **Proceedings of the 2006 workshop on New security paradigms NSPW '06**

**Publisher:** ACM Press

Full text available:  pdf(138.73 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Virtually every Internet user on the planet uses the powerful free tools offered by a handful of information service providers in many aspects of their personal and professional lives. As a result, users and organizations are freely providing unprecedented amounts of sensitive information in return for such services as Internet search, email, mapping, blog hosting, instant messaging and language translation. Traditional security measures, such as cryptography and network firewalls, are largel ...

**Keywords:** AOL, Google, anonymity, anonymization, fingerprinting, googling, information disclosure, privacy, search, usable security

Results 21 - 40 of 200

Result page: [previous](#) [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [next](#)

The ACM Portal is published by the Association for Computing Machinery. Copyright © 2007 ACM, Inc.

[Terms of Usage](#) [Privacy Policy](#) [Code of Ethics](#) [Contact Us](#)

Useful downloads:  [Adobe Acrobat](#)  [QuickTime](#)  [Windows Media Player](#)  [Real Player](#)



USPTO

[Subscribe](#) (Full Service) [Register](#) (Limited Service, Free) [Login](#)

 Search: ☒ The ACM Digital Library ☐ The Guide



THE ACM DIGITAL LIBRARY


[Feedback](#) [Report a problem](#) [Satisfaction survey](#)
Terms used: secure email message

Found 15,167 of 215,737

Sort results by

[Save results to a Binder](#)[Try an Advanced Search](#)

Display results

[Search Tips](#)[Try this search in The ACM Guide](#)
☐ Open results in a new window

Results 41 - 60 of 200

Result page: [previous](#) [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [next](#)

Best 200 shown

Relevance scale ☐ ☐ ☐ ☐ ☐**41** [Neuro-fuzzy applications: Active electronic mail](#)

S. Karnouskos, A. Vasilakos

March 2002 **Proceedings of the 2002 ACM symposium on Applied computing SAC '02**

Publisher: ACM Press

Full text available: [pdf\(532.13 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Network infrastructures have evolved tremendously over the last years, offering new capabilities to the applications in higher levels. Email is a widely used communication tool that could benefit of an intelligent and active underlying network in order to support sophisticated services. We explore in this paper an infrastructure based on intelligent mobile agents and active networks, and point out how and where advanced features can be introduced to our current passive email platform in order to ...

**Keywords:** active networks, computational intelligence, email, intelligent mobile agents**42** [The Yaksha security system](#)

Ravi Ganesan

March 1996 **Communications of the ACM**, Volume 39 Issue 3

Publisher: ACM Press

Full text available: [pdf\(3.90 MB\)](#) Additional Information: [full citation](#), [references](#), [citations](#), [index terms](#), [review](#)**43** [Inspiring teamwork & communication with a content management system](#)

Daniel B. Delgado

October 2007 **Proceedings of the 35th annual ACM SIGUCCS conference on User services SIGUCCS '07**

Publisher: ACM Press

Full text available: [pdf\(205.68 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Content Management Systems (CMS) take many shapes and forms and most are familiar with them. CMSs include everything from portals to blogs and wikis. Many organizations use CMS as websites to collate and organize information in readily available chunks. However, in a lab environment CMSs can increase teamwork and communications as well as stopping the knowledge drain as student employees graduate.

Before attending SIGUCCS '05, I led the development of many new online systems for the CIR ...


**Keywords:** AT, CIRCA, CMS, Daniel Delgado, UF, University of Florida, communication, content management system, deploying software systems, e107, requirements gathering, teamwork, technology consultants

44 Secure virtual private networks: the future of data communications

Eli Herscovitz

August 1999 **International Journal of Network Management**, Volume 9 Issue 4

**Publisher:** John Wiley & Sons, Inc.

Full text available:  [pdf\(230.05 KB\)](#) Additional Information: [full citation](#), [abstract](#), [index terms](#)

The Internet is an almost ideal means for Information retrieval and exchange. It is cost-effective, easy to use and easily accessible. However, it can also be susceptible to devious practices such as data tempering, eavesdropping and theft. This paper analyses secure virtual private networks &lpar;VPNs&rpar; and their use in countering the problems of the Internet. Copyright © 1999 John Wiley & Sons, Ltd.

45 Internet Privacy Enhanced Mail



Stephen T. Kent

August 1993 **Communications of the ACM**, Volume 36 Issue 8

**Publisher:** ACM Press

Full text available:  [pdf\(4.82 MB\)](#) Additional Information: [full citation](#), [references](#), [citations](#), [index terms](#), [review](#)

**Keywords:** Internet Privacy Enhanced Mail

46 Database privacy and security: Threats to privacy in the forensic analysis of database systems



Patrick Stahlberg, Gerome Miklau, Brian Neil Levine

June 2007 **Proceedings of the 2007 ACM SIGMOD international conference on Management of data SIGMOD '07**

**Publisher:** ACM Press

Full text available:  [pdf\(457.59 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

The use of any modern computer system leaves unintended traces of expired data and remnants of users' past activities. In this paper, we investigate the unintended persistence of data stored in database systems. This data can be recovered by forensic analysis, and it poses a threat to privacy.

First, we show how data remnants are preserved in database table storage, the transaction log, indexes, and other system components. Our evaluation of several real database systems reveals that d ...

**Keywords:** forensics, privacy, transparency

47 Cryptography: Chosen-ciphertext secure proxy re-encryption

Ran Canetti, Susan Hohenberger

October 2007 **Proceedings of the 14th ACM conference on Computer and communications security CCS '07**

**Publisher:** ACM

Full text available:  [pdf\(328.74 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

In a proxy re-encryption (PRE) scheme, a proxy is given special information that allows it to translate a ciphertext under one key into a ciphertext of the same message under a different key. The proxy cannot, however, learn anything about the messages encrypted under either key. PRE schemes have many practical applications, including distributed storage, email, and DRM. Previously proposed re-encryption schemes achieved only semantic security; in contrast, applications often require security ...


**Keywords:** chosen-ciphertext security, encryption, obfuscation, re-encryption

48 A taxonomy of computer program security flaws



Carl E. Landwehr, Alan R. Bull, John P. McDermott, William S. Choi  
September 1994 **ACM Computing Surveys (CSUR)**, Volume 26 Issue 3

**Publisher:** ACM Press

Full text available:  [pdf\(3.81 MB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#), [review](#)

An organized record of actual flaws can be useful to computer system designers, programmers, analysts, administrators, and users. This survey provides a taxonomy for computer program security flaws, with an Appendix that documents 50 actual security flaws. These flaws have all been described previously in the open literature, but in widely separated places. For those new to the field of computer security, they provide a good introduction to the characteristics of security flaws and how they ...

**Keywords:** error/defect classification, security flaw, taxonomy

49 NetNews: Fits and starts



Dennis Fowler  
December 2004 **netWorker**, Volume 8 Issue 4

**Publisher:** ACM Press

Full text available:  [pdf\(126.65 KB\)](#) Additional Information: [full citation](#), [index terms](#)  
 [html\(22.53 KB\)](#)

50 Pseudonyms and data privacy: The pynchon gate: a secure method of pseudonymous mail retrieval



Len Sassaman, Bram Cohen, Nick Mathewson  
November 2005 **Proceedings of the 2005 ACM workshop on Privacy in the electronic society WPES '05**

**Publisher:** ACM Press

Full text available:  [pdf\(306.60 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

We describe the Pynchon Gate, a practical pseudonymous message retrieval system. Our design uses a simple distributed-trust private information retrieval protocol to prevent adversaries from linking recipients to their pseudonyms, even when some of the infrastructure has been compromised. This approach resists global traffic analysis significantly better than existing deployed pseudonymous email solutions, at the cost of additional bandwidth. We examine security concerns raised by our model, and ...

**Keywords:** anonymity, mix networks, private information retrieval

**51** Search: Simple authentication for the web

Timothy W. van der Horst, Kent E. Seamons

May 2007 **Proceedings of the 16th international conference on World Wide Web WWW '07**

Publisher: ACM Press

Full text available: [pdf\(344.69 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Automated email-based password reestablishment (EBPR) is an efficient, cost-effective means to deal with forgotten passwords. In this technique, email providers authenticate users on behalf of web sites. This method works because web sites *trust* email providers to deliver messages to their intended recipients. Simple Authentication for the Web (SAW) improves upon this basic approach to user authentication to create an alternative to password-based logins. SAW: 1) Removes the setup and ...

**Keywords:** authentication, password alternative, web single sign-on**52** Protecting applications with transient authentication

Mark D. Corner, Brian D. Noble

May 2003 **Proceedings of the 1st international conference on Mobile systems, applications and services MobiSys '03**

Publisher: ACM Press

Full text available: [pdf\(294.40 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [cited by](#)

How does a machine know who is using it? Current systems authenticate their users infrequently, and assume the user's identity does not change. Such *persistent authentication* is inappropriate for mobile and ubiquitous systems, where associations between people and devices are fluid and unpredictable. We solve this problem with *Transient Authentication*, in which a small hardware token continuously authenticates the user's presence over a short-range, wireless link. We present the fo ...

**53** Computer security (SEC): SELS: a secure e-mail list service

Himanshu Khurana, Adam Slagell, Rafael Bonilla

March 2005 **Proceedings of the 2005 ACM symposium on Applied computing SAC '05**

Publisher: ACM Press

Full text available: [pdf\(218.91 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

Exchange of private information content among a large number of users via *E-mail List Services* is becoming increasingly common. In this paper we address security requirements in that setting and develop a new protocol, SELS (a Secure E-mail List Service) that provides confidentiality, integrity, and authentication for e-mails exchanged via lists. In addition, SELS also protects against the use of lists for e-mail spamming. We have developed a prototype of SELS in Java, and integrated it w ...

**Keywords:** electronic mail, mailing list, security**54** Crypto-based identifiers (CBIDs): Concepts and applications

Gabriel Montenegro, Claude Castelluccia

February 2004 **ACM Transactions on Information and System Security (TISSEC)**, Volume 7 Issue 1

Publisher: ACM Press

Full text available: [pdf\(262.76 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#), [review](#)

This paper addresses the identifier ownership problem. It does so by using characteristics of Statistical Uniqueness and Cryptographic Verifiability (SUCV) of certain entities which



this document calls SUCV Identifiers and Addresses, or, alternatively, Crypto-based Identifiers. Their characteristics allow them to severely limit certain classes of denial-of-service attacks and hijacking attacks. SUCV addresses are particularly applicable to solve the address ownership problem that hinders mechani ...

**Keywords:** Security, address ownership, authorization, group management, mobile IPv6, opportunistic encryption

55 Teaching secure communication protocols using a game representation

Leonard G. C. Hamey

January 2003 **Proceedings of the fifth Australasian conference on Computing education - Volume 20 ACE '03**

**Publisher:** Australian Computer Society, Inc.

Full text available:  [pdf\(252.19 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

The Security Protocol Game is a highly visual and interactive game for teaching secure data communication protocols. Students use the game to simulate protocols and explore possible attacks against them. The power of the game lies in the representation of secret and public key cryptography. Specifically, the game provides representations for plain text and encrypted messages, message digests, digital signatures and cryptographic keys. Using these representations, students can construct public ke ...

**Keywords:** PGP, blind signature, computer network, cryptography, digital signature, key exchange, man-in-the-middle attack, protocols, replay attack, secure communication


56 Towards junking the PBX: deploying IP telephony



Wenyu Jiang, Jonathan Lennox, Henning Schulzrinne, Kundan Singh

January 2001 **Proceedings of the 11th international workshop on Network and operating systems support for digital audio and video NOSSDAV '01**

**Publisher:** ACM Press

Full text available:  [pdf\(312.40 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

We describe the architecture and implementation of our Internet telephony test-bed intended to replace the departmental PBX (telephone switch). It interworks with the traditional telephone networks via a PSTN/IP gateway. It also serves as a corporate or campus infrastructure for existing and future services like web, email, video and streaming media. Initially intended for a few users, it will eventually replace the plain old telephones from our offices, due to the cost benefit and new ...

**Keywords:** PSTN/IP interoperability, SIP, VoIP test-bed, internet telephony deployment

57 VizSEC short papers session: Email archive analysis through graphical visualization



Wei-Jen Li, Shlomo HersHKop, Salvatore J. Stolfo

October 2004 **Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security VizSEC/DMSEC '04**

**Publisher:** ACM Press

Full text available:  [pdf\(403.73 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

The analysis of the vast storehouse of email content accumulated or produced by individual users has received relatively little attention other than for specific tasks such as spam and virus filtering. Current email analysis in standard client applications consists of keyword based matching techniques for filtering and expert driven manual exploration of email files.

We have implemented a tool, called the Email Mining Toolkit (EMT) for analyzing email archives which includes a graphic ...

**Keywords:** email, spam, virus

58 Secure key issuing in ID-based cryptography

Byoungcheon Lee, Colin Boyd, Ed Dawson, Kwangjo Kim, Jeongmo Yang, Seungjae Yoo  
January 2004 **Proceedings of the second workshop on Australasian information security, Data Mining and Web Intelligence, and Software Internationalisation - Volume 32 ACSW Frontiers '04**

**Publisher:** Australian Computer Society, Inc.

Full text available:  [pdf\(177.95 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

ID-based cryptosystems have many advantages over PKI based cryptosystems in key distribution, but they also have an inherent drawback of key escrow problem, i.e. users' private keys are known to the key generation center (KGC). Therefore secure key issuing (SKI) is an important issue in ID-based cryptography. In multiple authority approach (Boneh & Franklin 2001, Chen et al. 2002), key generation function is distributed to multiple authorities. Keeping key privacy using user-chosen secret inform ...

**Keywords:** ID-based cryptography, bilinear pairing, blinding, key generation center (KGC), key privacy authority (KPA), secure key issuing (SKI)

59 Securing the global, remote, mobile user

Walt Curtis, Lori Sinton

March 1999 **International Journal of Network Management**, Volume 9 Issue 1

**Publisher:** John Wiley & Sons, Inc.

Full text available:  [pdf\(982.14 KB\)](#) Additional Information: [full citation](#), [abstract](#), [index terms](#)

Electronic commerce is inevitable and will reshape our lives, but before true electronic commerce environments can be realized, it will be necessary to secure your enterprise against outside attacks on its electronic information and provide controls for authorized access to that information. Copyright © 1999 John Wiley & Sons, Ltd.

60 Security for diffuse computing: Securing publish-subscribe overlay services with EventGuard

Mudhakar Srivatsa, Ling Liu

November 2005 **Proceedings of the 12th ACM conference on Computer and communications security CCS '05**

**Publisher:** ACM Press

Full text available:  [pdf\(488.84 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

A publish-subscribe overlay service is a wide-area communication infrastructure that enables information dissemination across geographically scattered and potentially unlimited number of publishers and subscribers. A wide-area publish-subscribe (pub-sub) system is often implemented as a collection of spatially disparate nodes communicating on top of a peer to peer overlay network. Such a model presents many inherent benefits such as scalability and performance, as well as potential challenges su ...

Useful downloads:  [Adobe Acrobat](#)  [QuickTime](#)  [Windows Media Player](#)  [Real Player](#)